

Open DNS Resolver Check Site

Hiroshi KOBAYASHI, Takayuki UCHIYAMA
Japan Computer Emergency Response Team
Coordination Center (JPCERT/CC)

Agenda

■ Background

- History

■ Mechanism

- Work Diagram

- Countermeasure

■ Statistics

- Access History

■ Collaboration

- Domestic

- International

Hiroshi KOBAYASHI

koba is a Information Security Analyst at JPCERT Coordination Center, National CSIRT in Japan.

He is in charge of incident response.

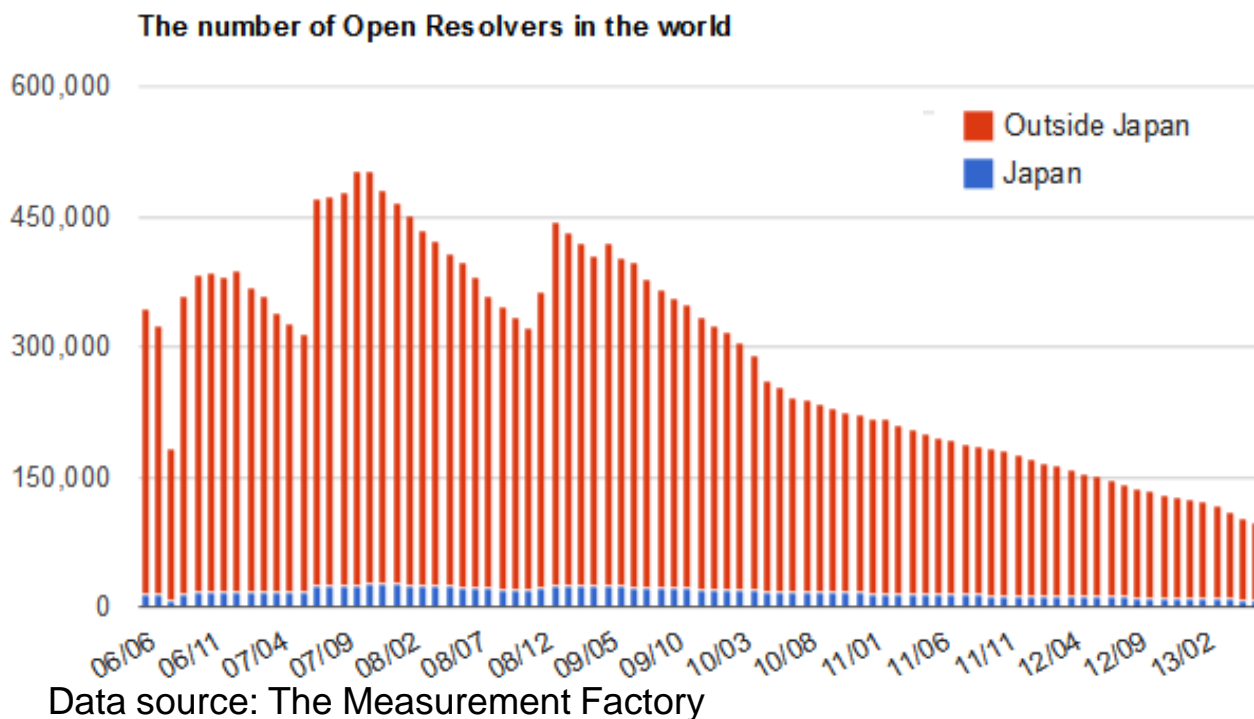
Takayuki UCHIYAMA

Taki is a Information Security Analyst at JPCERT Coordination Center, National CSIRT in Japan.

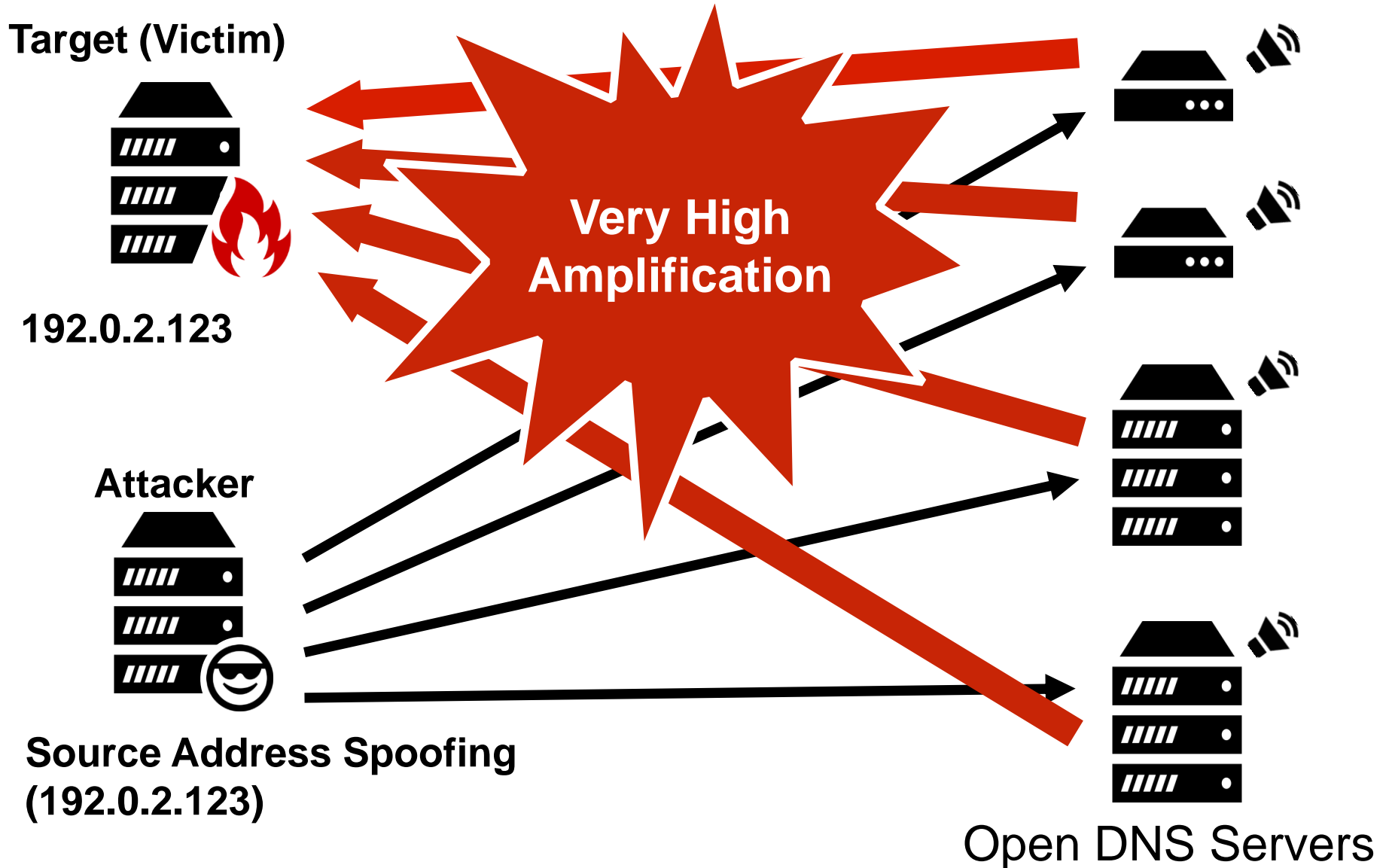
He is in charge of handling vulnerability reports.

Open DNS Resolver Issue

- Open DNS resolver issue has been a persistent issue for quite a long period of time.
 - It was a big topic around 2006
- The number of open resolver hosts (since 2006) is shown at The Measurement Factory website.



DNS Amplification Attack



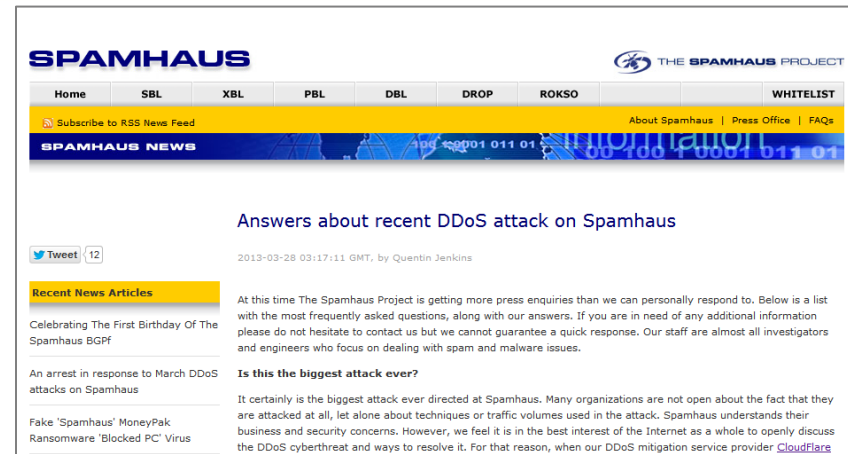
Open Resolver Issue in 2013

■ Spamhaus

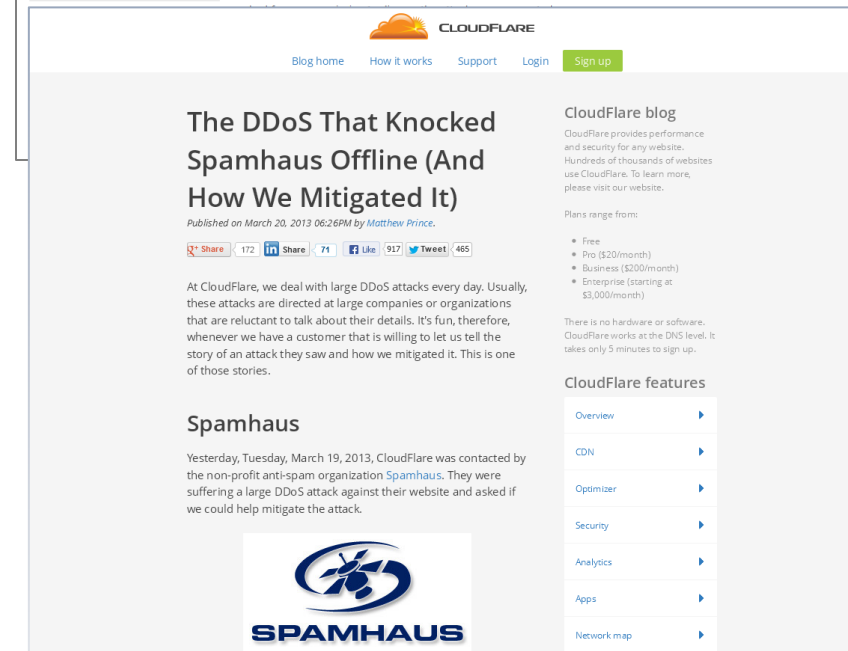
- From 19/Mar/2013
- Over 300Gbps during 1 week span!?
- Reported by CloudFlare

■ JPCERT/CC continues to receive many incident reports.

■ Small-scale DNS attacks are observed regularly in Japan.



The screenshot shows the Spamhaus website header with navigation links: Home, SBL, XBL, PBL, DBL, DROP, ROKSO, and WHITELIST. Below the header is a yellow banner with 'Subscribe to RSS News Feed' and 'About Spamhaus | Press Office | FAQs'. The main content area features a blue banner with 'SPAMHAUS NEWS' and a date '19 Mar 2013 01:11:01'. The article title is 'Answers about recent DDoS attack on Spamhaus', dated '2013-03-28 03:17:11 GMT, by Quentin Jenkins'. The article text discusses the project's response to press enquiries and mentions a 'biggest attack ever?'.



The screenshot shows the CloudFlare blog post. The title is 'The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)', published on March 20, 2013, 06:26PM by Matthew Prince. The post includes social sharing buttons for Google+, LinkedIn, Facebook, and Twitter. The text describes how CloudFlare handles large DDoS attacks and mentions that Spamhaus was contacted by the non-profit anti-spam organization Spamhaus. The CloudFlare logo is visible at the bottom of the post.

Motivation for the check site

- Responsibility to protect our constituents!
- JPCERT/CC Initial Actions
 - Notification
 - Sent notifications to the appropriate contacts of Open Resolver hosts
 - Types of organizations / service providers contacted
 - User hosts on the hosting service
 - User hosts on the home
 - DNS servers on the enterprise environment
 - ISP DNS cache servers

Motivation for the check site

- Open Resolver hosts on the hosting service
 - Hosts often do NOT NEED to run a DNS server.
- Many host administrators are not aware of running DNS service on their own hosts.
 - Default Packages
 - OS image templates include DNS service as a server.
 - Software packages are delivered with Management Software that include DNS server components.
- Contacted individuals may be inappropriate for handling such an issue
- It is hard to get a good contact that can properly address the issue

Motivation for the check site

- openresolver.jp
 - Contacted Organizations
 - User hosts on the hosting service
 - User hosts on the home, ISP
 - It can be extremely difficult for administrators/users to recognize if their host server/device is an open resolver or not.
 - There are many similar open resolver check sites, but our site offers:
 - An easy and simple method
 - Increased awareness towards the open resolver issue to users that visit the site.

Open Resolver check site has been released

オープンリゾルバ確認サイト

<http://www.openresolver.jp/>

JPCERT/CC では、オープンリゾルバとなっている DNS サーバが日本国内に多く存在していることを確認しています。また独自の調査を行っている [Open Resolver Project](#) によると、世界全体で約 2800万 (2013/10末現在) のオープンリゾルバが存在すると報告されています。

オープンリゾルバとは、外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS サーバのことです。オープンリゾルバは国内外に多数存在し、大規模な DDoS 攻撃の踏み台として悪用されているとの報告があります。

また、DNS サーバとして運用しているホストだけではなく、ブロードバンドルータなどのネットワーク機器が意図せずオープンリゾルバになっている事例があることを確認しています。

本確認サイトでは、お使いの PC に設定されている DNS サーバと、本確認サイトへの接続元となっているブロードバンドルータなどのネットワーク機器がオープンリゾルバとなっていないかを確認することが可能です。

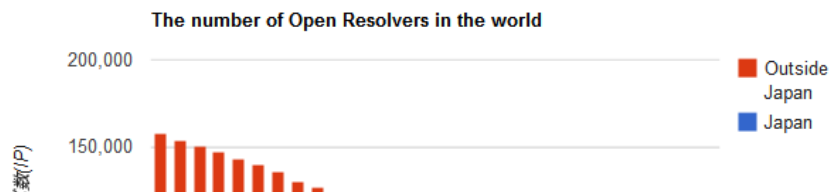
本サイトを活用し、健全なインターネット運用にご協力いただけますようお願いいたします。

ホスティングサービスで使用しているサーバがユーザの意図しないままオープンリゾルバとなっている事象も多く報告されています。これらのホスト管理者の方が `wget` コマンドなどを使用してコマンドラインから確認できるサイトも用意しています。

コマンドラインからの [確認方法](#)

※ 本サイトの公開時から2013年10月31日14時58分の間において、オープンリゾルバの可能性がある場合に表示される「設定されているDNSサーバ」と「接続元IPアドレス」のIPアドレスの結果に誤りがありました。誠に申し訳ございませんが、再度確認いただけますようお願いいたします。

★ 本サイトの詳細については [こちら](#) をご参照ください。



Also available in English

Open DNS Resolver Check Site

<http://www.openresolver.jp/en/>

JPCERT/CC has been observing situations where open DNS resolvers are spread widely across Japan. Moreover, according to the survey conducted by the [Open Resolver Project](#), there exist about 28 million open DNS resolvers throughout the world (as of Oct 2013).

An open DNS resolver is a publicly accessible name server that provides a recursive name resolution for unspecified IP addresses. It has been reported that a number of open DNS resolvers are being exploited to participate in massive distributed denial of service (DDoS) attacks.

JPCERT/CC has also been observing situations where not only host computers that operate as DNS servers but also network devices (e.g. broadband routers) unintentionally running open DNS resolvers.

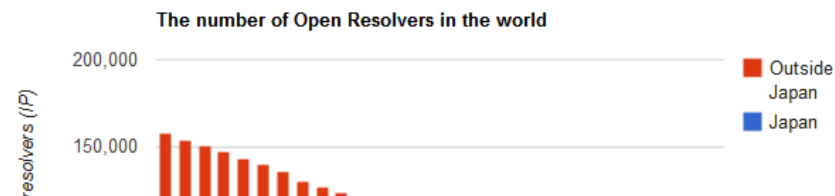
This site allows you to check on the following 2 points:

- Whether the DNS server configured on your PC is running an open DNS resolver or not
- Whether your network device (e.g. broadband router) connecting to this site is running an open DNS resolver or not

JPCERT/CC appreciates your contribution towards a robust cyber space by utilizing this check site.

JPCERT/CC has also received a number of reports where servers of hosting services are operating as open DNS resolvers, despite users' intentions. We have also set up another site for such host administrators to check their computers using command lines (e.g. "wget" command).

Try check site using command lines at the following URL:
<http://www.openresolver.jp/cli/check.html>



Command line tool is also available

For those that cannot check using a web browser, we have prepared a command based tool:

wget:

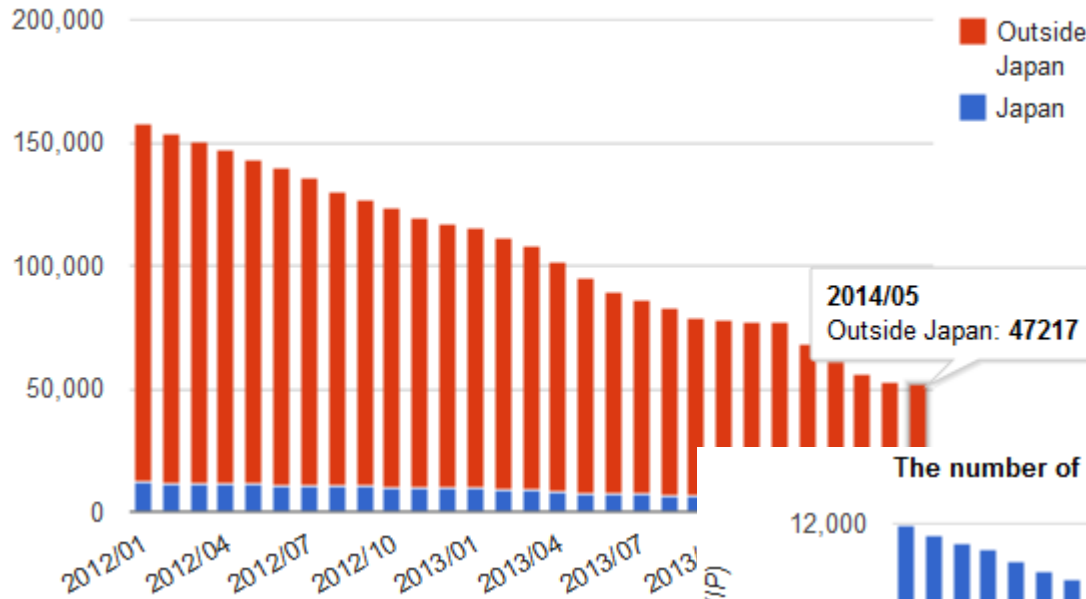
```
$ wget -qO - http://www.openresolver.jp/cli/check.html  
Configured DNS server: [OPEN] 192.0.2.2(ns.example.com)  
Source IP address: [NOT open] 192.0.2.1(gw.example.com)
```

curl :

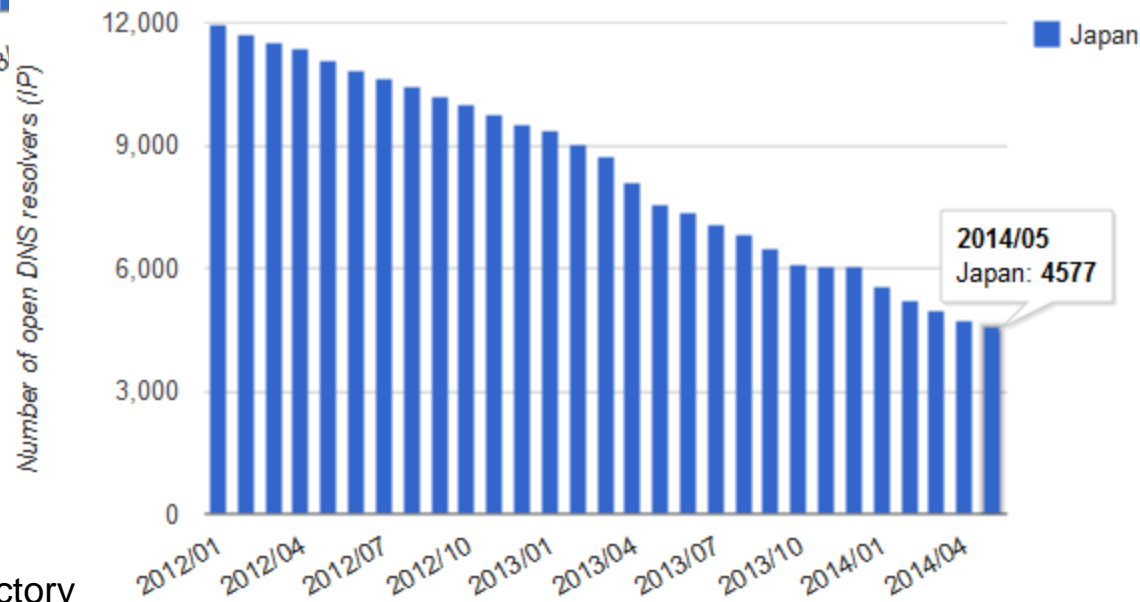
```
$ curl --location-trusted http://www.openresolver.jp/cli/check.html  
Configured DNS server: [OPEN] 192.0.2.2(ns.example.com)  
Source IP address: [NOT open] 192.0.2.1(gw.example.com)
```

The Measurement Factory Statistics

The number of Open Resolvers in the world



The number of Open Resolvers in Japan

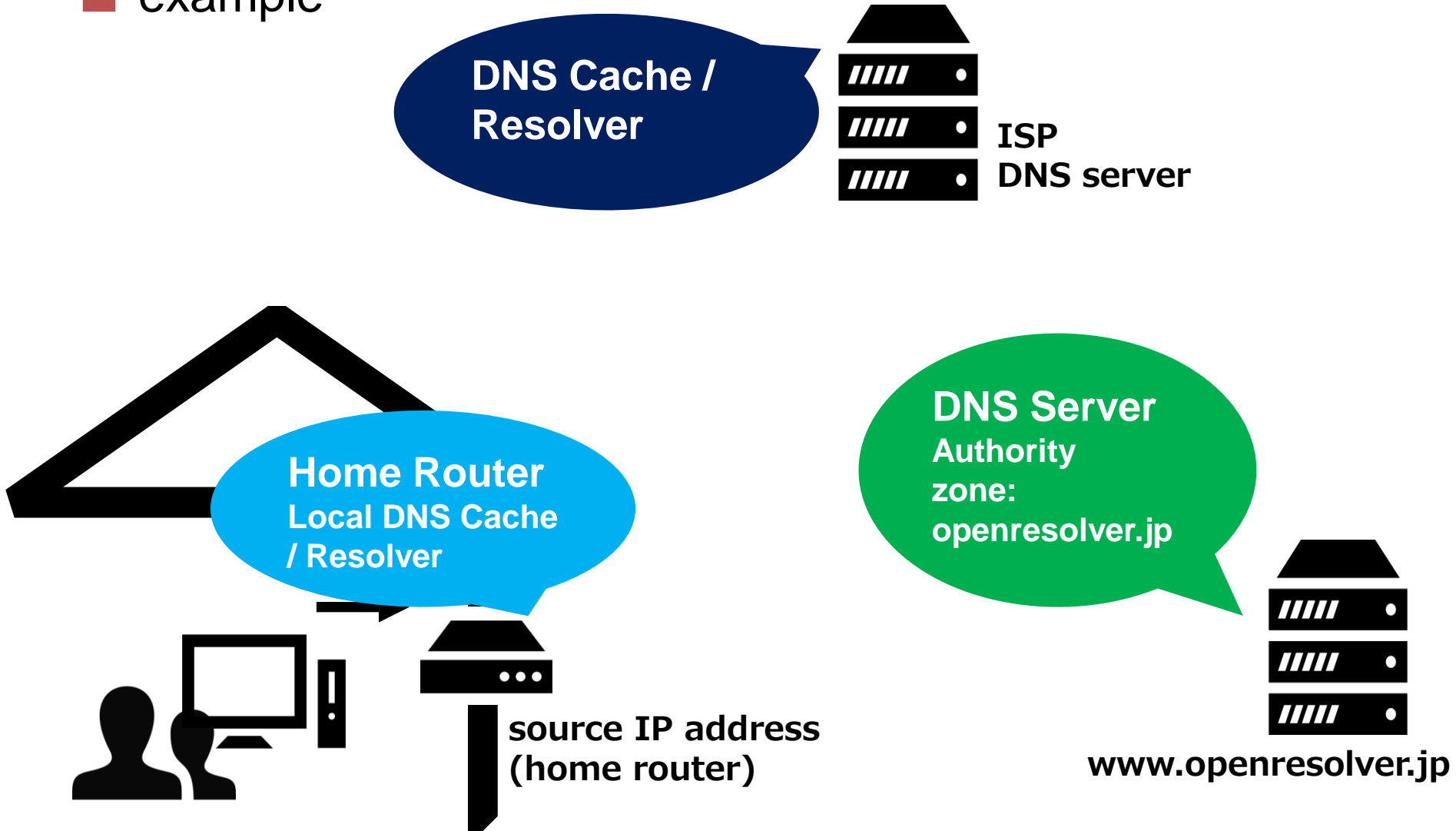


These graphs
are also
available at
openresolver.jp

Data source: The Measurement Factory

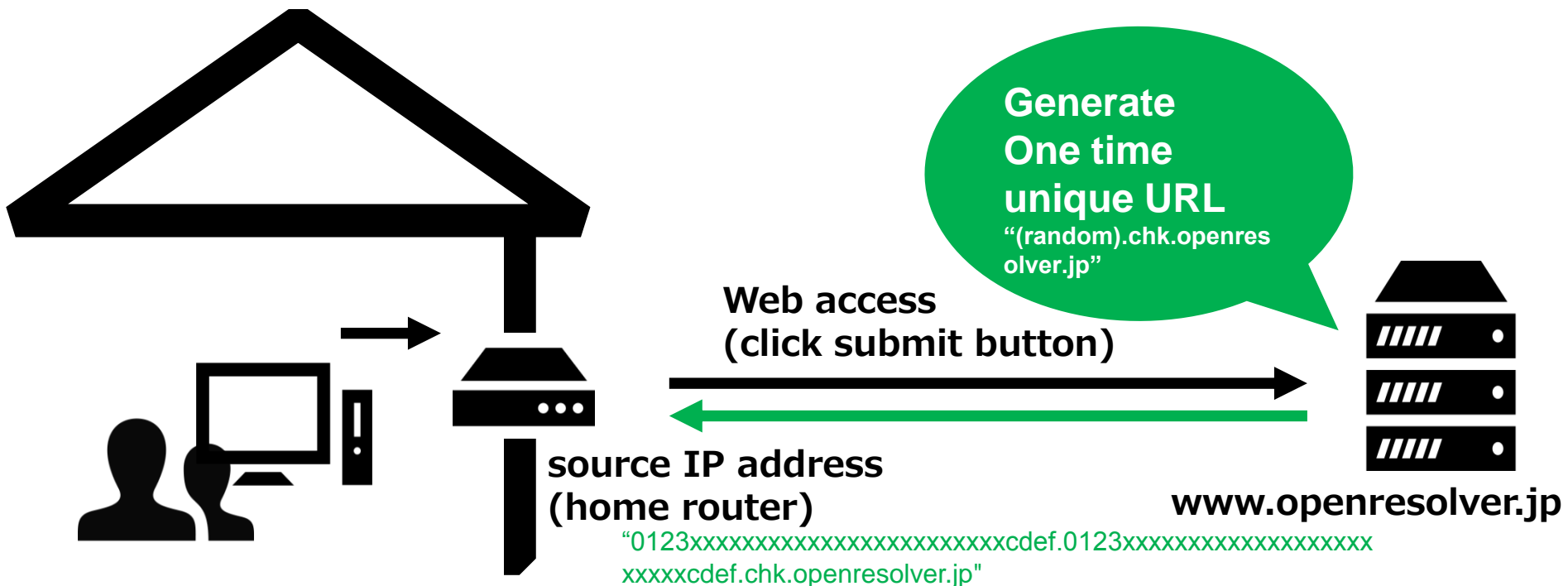
How openresolver.jp Works

■ example



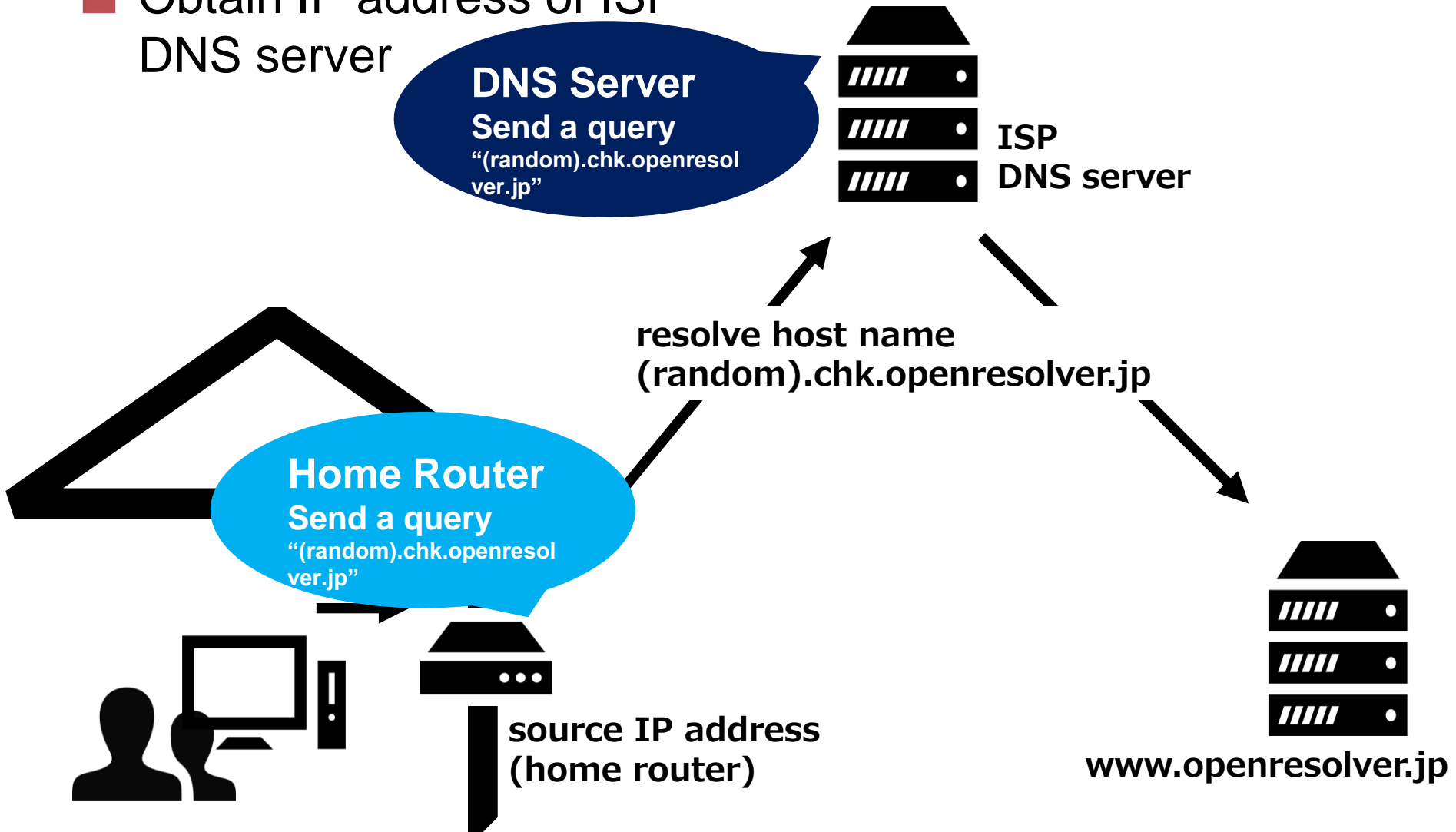
How openresolver.jp Works

- Click “Submit” on the Agreement page



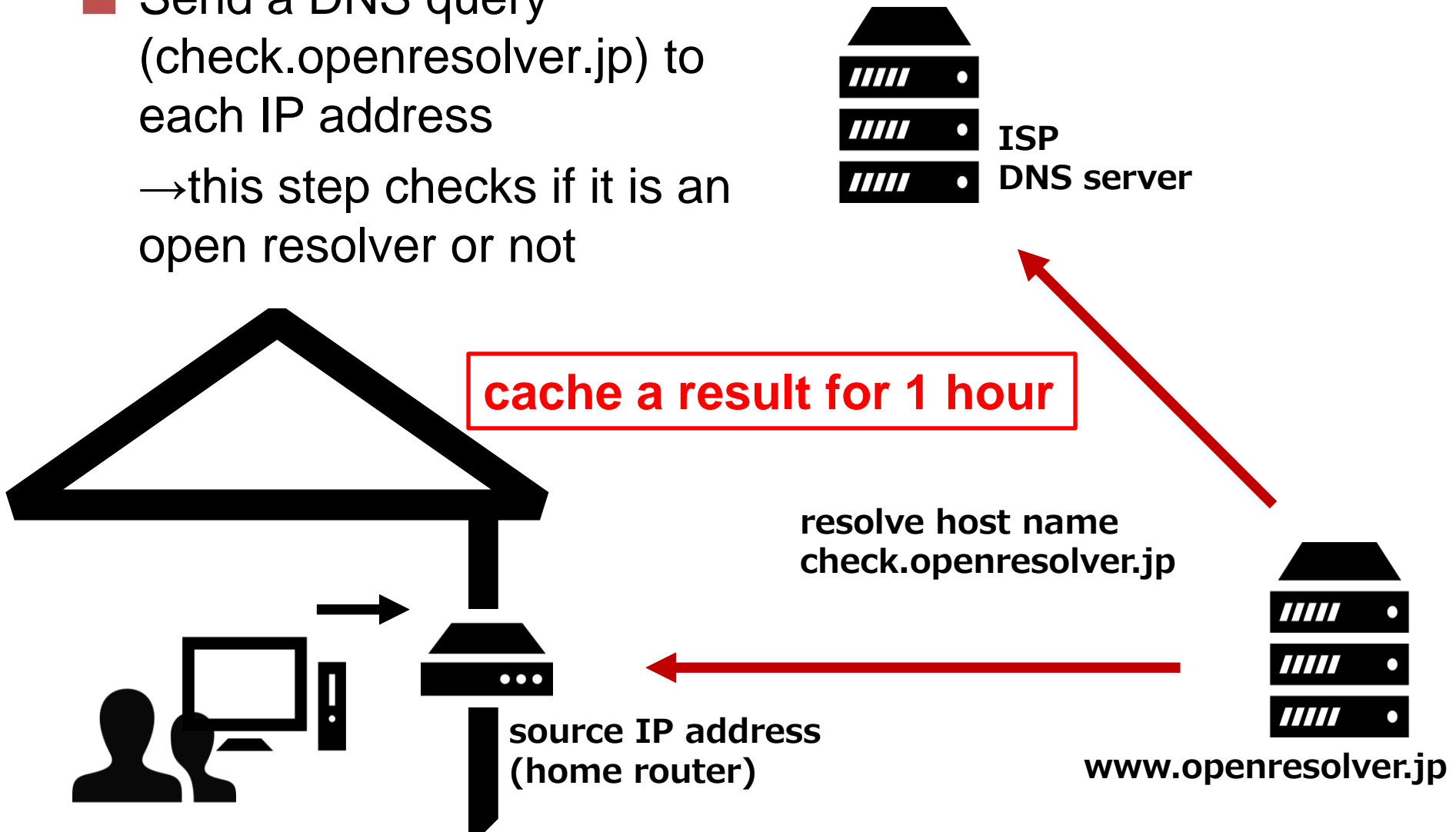
How openresolver.jp Works

- Obtain IP address of ISP DNS server



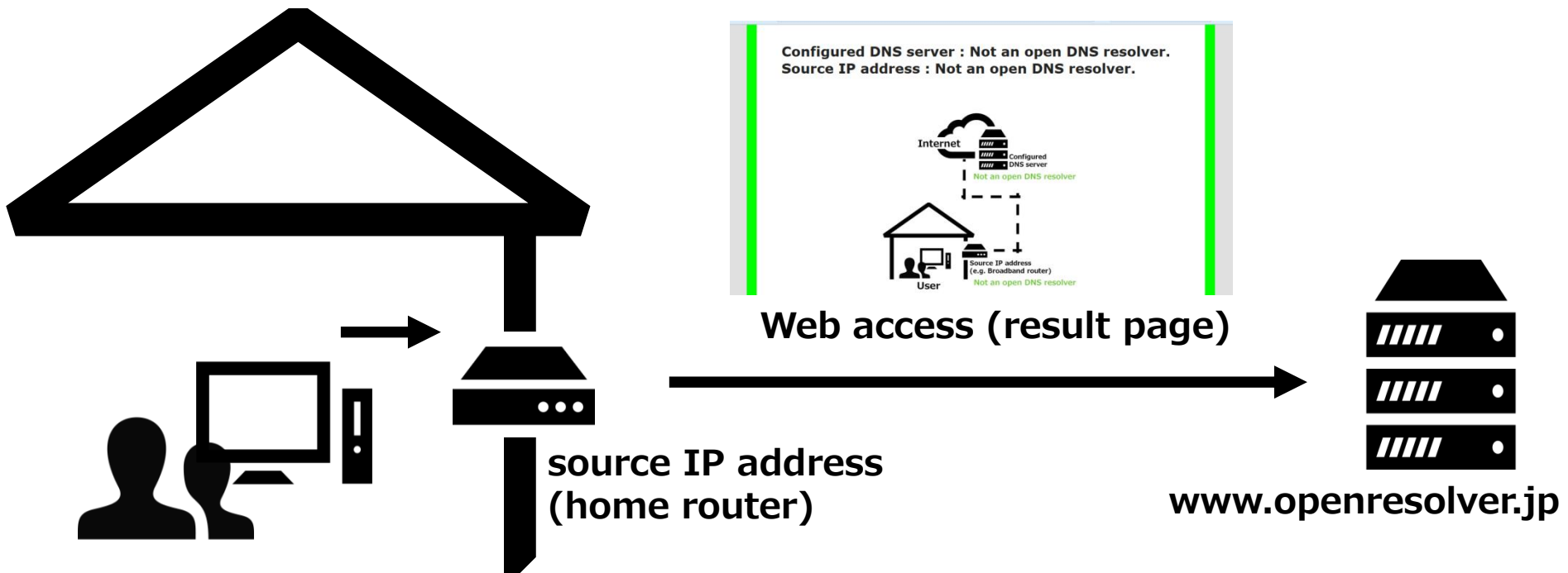
How openresolver.jp Works

- Send a DNS query (check.openresolver.jp) to each IP address
→this step checks if it is an open resolver or not



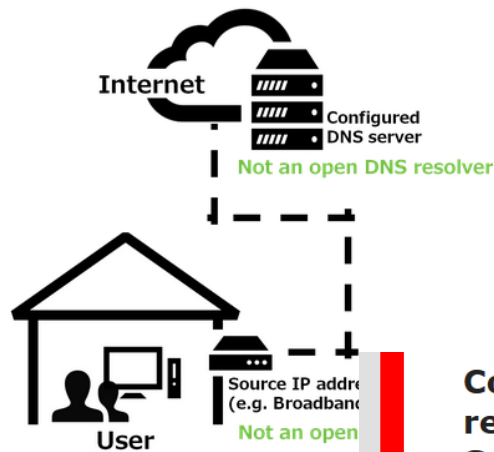
How openresolver.jp Works

- Obtain source IP address

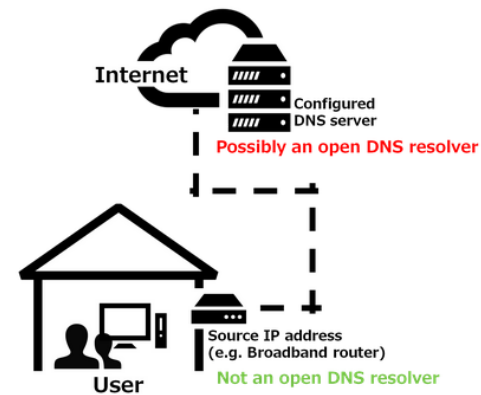


Sample result page

Configured DNS server : Not an open DNS resolver.
Source IP address : Not an open DNS resolver.



Configured DNS server : Possibly an open DNS resolver.
Source IP address : Not an open DNS resolver.



Instruction for openresolver users

- Visitors can also follow the instructions to address the issue
- Countermeasure process
 - Configure DNS appropriately
 - Send the check results to JPCERT/CC
 - Home Router brand name, version and etc.
 - Useful links on additional technical information

III. 対策

(1) 設定されている DNS サーバがオープンリゾルバと判定されたとき

— ご自身 (もしくは自組織) の管理する DNS サーバの場合

1) DNS サーバの設定を見直すことをご検討ください。

JPRS

DNSサーバの不適切な設定「オープンリゾルバ」について
<http://jprs.jp/important/2013/130418.html>

JPNIC

オープンリゾルバ (Open Resolver) に対する注意喚起
<https://www.nic.ad.jp/ja/dns/openresolver/>

— 上記以外の場合 (プロバイダの DNS サーバなど)

1) JPCERT/CC より管理者の方へご連絡いたしますので、JPCERT/CC への報告をご検討ください。

JPCERT/CC

インシデントの報告
<https://form.jpCERT.or.jp/>

「インシデントの報告」をクリックして、「情報提供」を選択いただき、以下項目を記載の上、「ご要望の記入欄」にご記入いただけますようお願い申し上げます。

記入例は [こちら](#) です。

—

当該 DNS サーバの IP アドレス:
当該 DNS サーバを設定した経緯:

—

(2) 接続元の IP アドレスがオープンリゾルバと判定されたとき

— 該当の IP アドレスがブロードバンドルータなどのネットワーク機器の場合

1) お使いのブロードバンドルータなどのネットワーク機器の設定や、最新のソフトウェアバージョンをお使いかどうかを確認してください。
※ 製品の取り扱い方法については、メーカーのマニュアルやサポートサイト等をご参照ください。

Japan Vulnerability Notes JVN#62507275

複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
<https://jvn.jp/jp/JVN62507275/index.html>

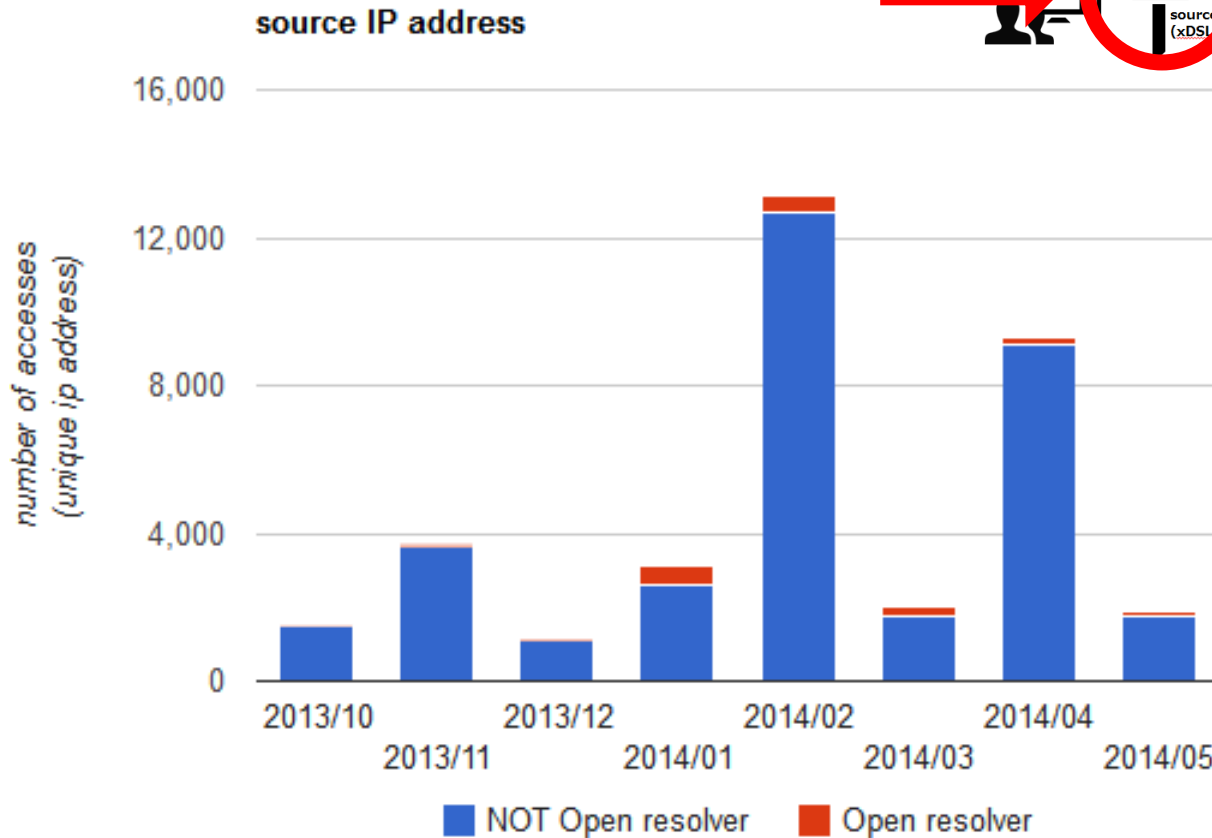
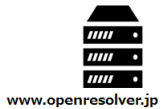
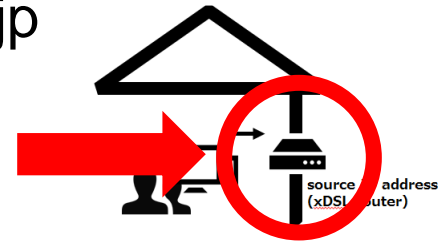
Japanese site

Openresolver.jp Statistics

■ Statistics

— Site Access to www.openresolver.jp

■ Source device (Home Router)

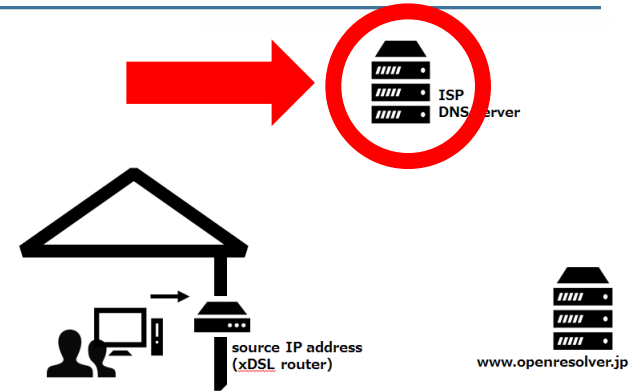
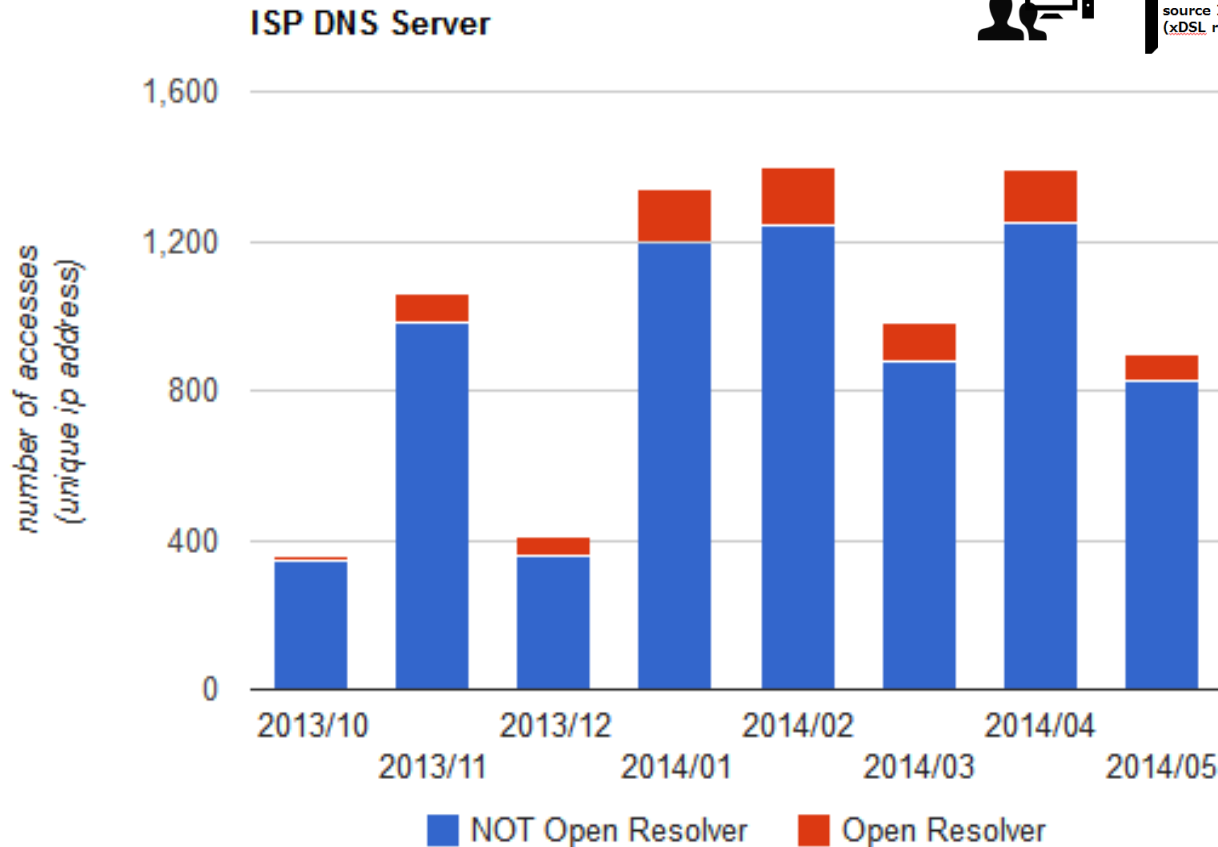


Openresolver.jp Statistics

■ Statistics

— Site Access to www.openresolver.jp

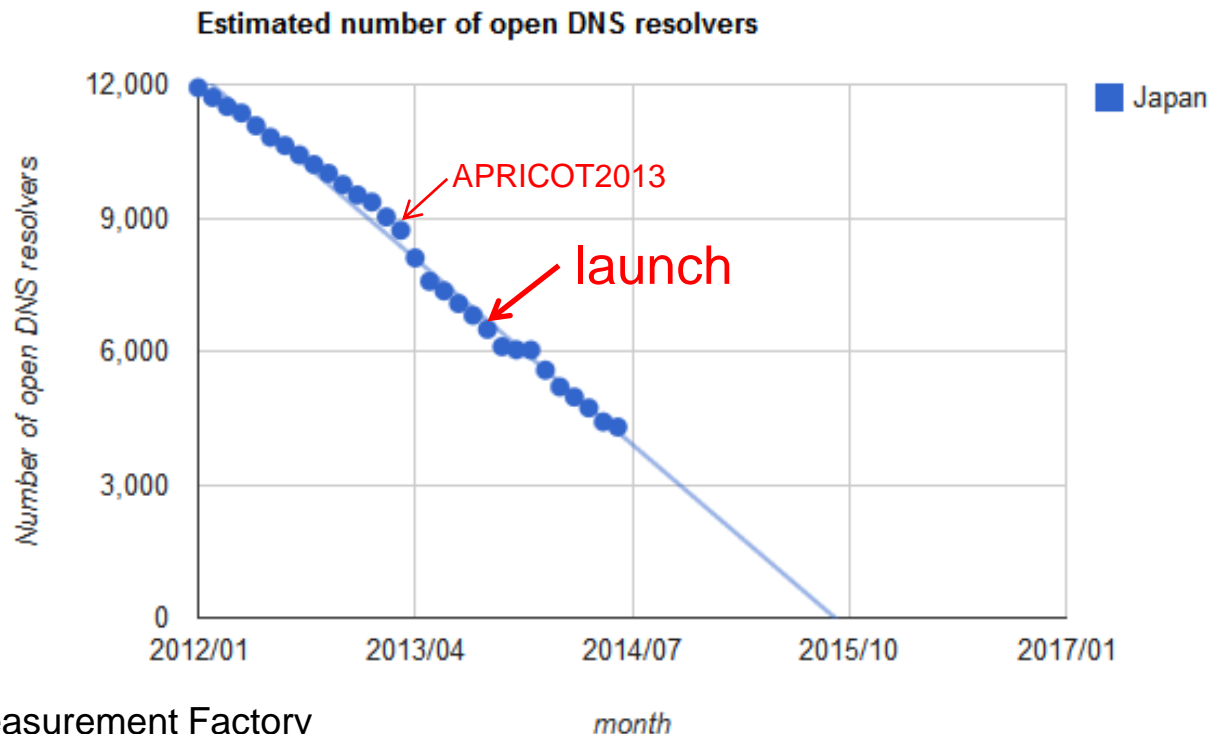
■ ISP DNS Server



Conclusion – Results obtained from the site

■ According to MF

- The number of Open Resolver hosts continues to decrease
- If this pace holds up, we have hope that this issue may be cleared up in 4 years
 - Of course, we would like it to be addressed sooner!



Data source: The Measurement Factory

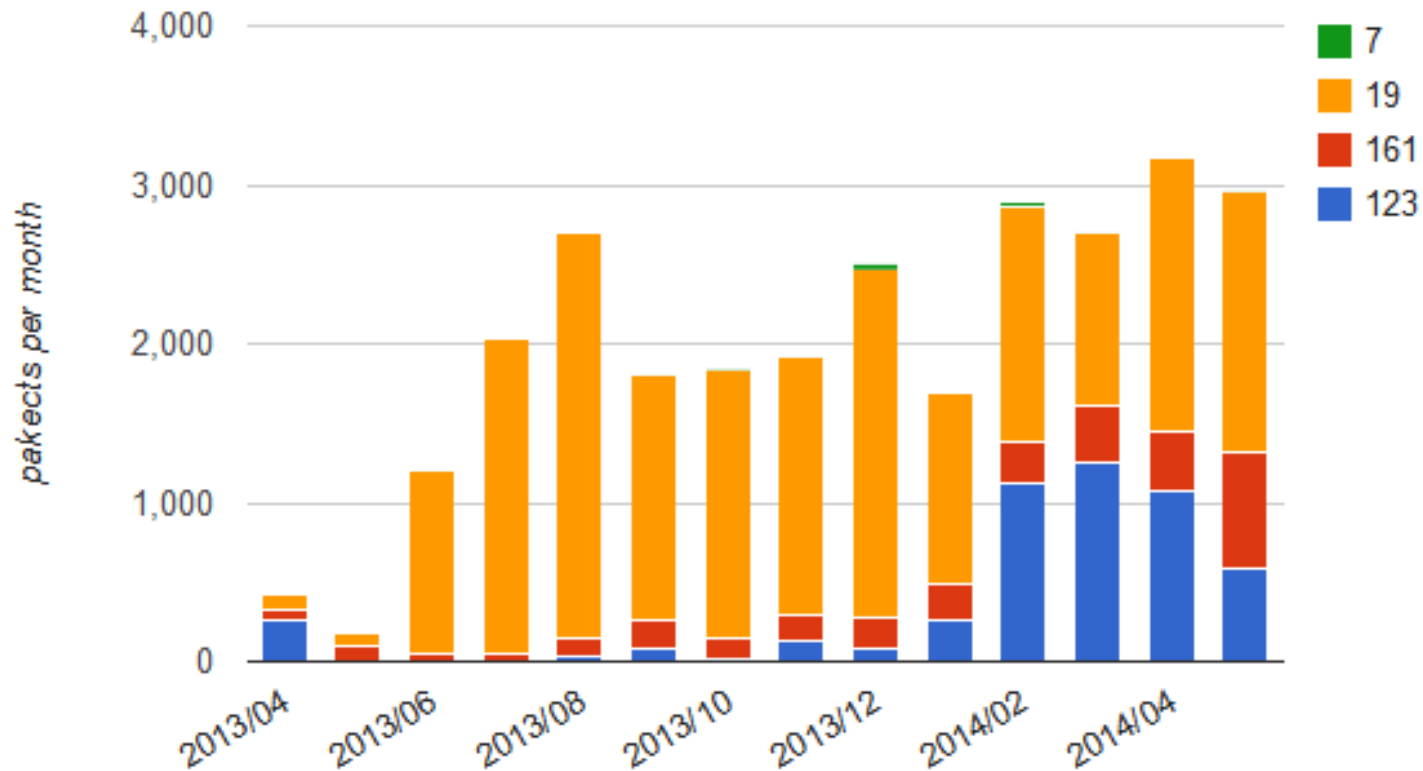
In the future...

- Wishful thinking says that as use of our site increases (along with other available sites) the number of open resolvers will decrease
 - But in reality, just “using” the site will not decrease the number of open resolvers
 - Countermeasures need to be put in place to eliminate the open resolvers
 - In some cases coordination is necessary
- JPCERT/CC will continue its efforts to address this issue domestically and will collaborate with any global partners that need assistance with this issue

Recent DDoS Trends

■ Other UDP protocols other than DNS

—123/udp (ntp), 161/udp (snmp), 19/udp (chargen),
7/udp(echo)



Contact Information

Home

- サイト内検索
- 検索
- トップページ
- 情報提供
 - 注意喚起
 - 早期警戒
 - 脆弱性対策情報
 - Weekly Report
- 各種届出・申込
- 制御システムセキュリティ
- ラーニング
- 公開資料
 - 四半期レポート
 - 研究・調査レポート
 - CSIRTマテリアル
- イベント
- プレスリリース
- JPCERT/CC

関連組織



JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。



JPCERT/CCはAPCERTの事務協力をしています。

General Contact

— Email : office@jpcert.or.jp

— Tel : +81.3.3518.4600

— <https://www.jpcert.or.jp>

Incident Reporting

— Email : info@jpcert.or.jp

— PGP Public Key :
<https://www.jpcert.or.jp/english/ir/pgp.html>

— Incident Reporting Form :
<https://www.jpcert.or.jp/english/ir/form.html>

Weekly Report

HTTPS RSS

セキュリティインシデント...
フィッシングサイト...
Webサイトの改ざん...
マルウェア...
不正アクセス...

発生元への「調整」を依頼したい
インシデントを「報告」したい

ISDAS
[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

お薦めページ

セキュリティ対策講座

教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント

- 第21回 FIRST Annual Conference 京都 参加申し込み受付中
- O/O+ セキュアコーディング ハーフデイキャンプ参加申し込み